RESPONSE TO THE MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS' REQUEST FOR FEEDBACK ON THE PROPOSED DATA PROTECTION REGIME FOR SINGAPORE

WONGPARTNERSHIP LLP
One George Street
#20-01
Singapore 049145
Tel: + 65 6416 8000
Fax: +65 6532 5711/+65 6532 5722
Email: contactus@wongpartnership.com
Website: www.wongpartnership.com

RESPONSE TO THE MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS' REQUEST FOR FEEDBACK ON THE PROPOSED DATA PROTECTION REGIME FOR SINGAPORE

1. DEFINITION OF "PERSONAL DATA"

1.1. In Question 3, The Ministry of Information, Communications and the Arts ("**MICA**") has asked:

> "Do you have any views/comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?"

1.2 We note that the proposed definition: "personal data" means information about an identified or identifiable individual; where "individual" means a natural person, whether living or deceased is similar to the broad definition of "personal data" that has been applied in other commonwealth jurisdictions such as the United Kingdom and Australia.

1.3 There is certainly merit in the notion of the Australian concept that personal information could include information from which the identity "can reasonably be ascertained" (see the definition of "personal information" at section 6 of the Australian Privacy Act 1988 [Act No. 119 of 1988] in the attached **Annex**). If such an approach was to be followed in Singapore, one suggestion is that information about an identifiable individual could be qualified as being information that could include data which with "reasonable effort or inquiry using public information" could lead a third party to ascertain the identity of an individual. The element of there being "reasonable" effort or inquiry combined with the use of "public information" could provide a needed degree of flexibility to qualify information which may be deemed as "personal data" without penalizing businesses or organisations with onerous obligations.

1.4 Whilst there is much to be said for having a broad definition such as the definitions adopted in the United Kingdom and Australia, another view is that perhaps Singapore could follow an approach such as that adopted in Canada, where categories of information covered by the definition of "personal data" are more specifically defined (see the definition of "personal information" at section 3 of the Canadian Privacy Act [R.S.C.,1985,c. P-21] in the attached **Annex**).

1.5 Another suggestion is that an express savings could be included in the definition to exclude information that has been aggregated, or where individual data subjects[1] are not identifiable or referenceable. As there have been some discussions in other jurisdictions about whether an IP address can be considered "personal data", this problem could be addressed in Singapore where indirect referencing is caught within the definition of "personal data" only where the reference databases are publicly available.

1.6 At Question 4, MICA has asked:

[1] In this response, "data subject" refers to the person to whom the data relates. This may be a different person from the person entering or providing the information.

> "With reference to paragraphs 3.15 to 3.16, do you have any views/comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views/comments on the proposed approach to the protection of personal data of the deceased?"

1.7 With respect to the personal information of deceased individuals, our comment is that any exemption of the information of deceased individuals from the regime should be qualified in scenarios where the information concerning the deceased individual may potentially result in the disclosure of personal information relating to a living individual. Any such qualification to the exemption could take into account the proposal suggested in paragraph 1.3 concerning "reasonable effort or inquiry using public information" which could allow the regime to strike a balance in connection with this concern. To take an example, the proposed legislation may be applied to protect the particulars of the next of kin of a particular deceased individual except for such information on the next of kin as is already public information.

2. TYPES OF ORGANISATIONS AND ACTIVITIES COVERED

2.1. In Question 5, MICA has asked:

> "Do you have any views/comments on the proposed organisations covered by the DP Law?"

2.2 Although there are numerous policy considerations in the proposed exclusion of the public sector from the proposed law, there is merit in the idea of providing a clarificatory provision that the lawfully excepted public use or disclosure of personal information by a public sector body should not, in and of itself, be used as a basis for the treatment of that information as public information by a person in the private sector. This is to ensure that the exemption of the public sector from the regime does not, in turn, impact the classification of data as personal information simply because of the fact that it is used in the course of the excepted activities of the public sector. In this respect, this qualification could be important in connection with addressing the proposed exclusion of "data under control of a public agency".

2.3 In Question 6, MICA has asked:

> "With reference to paragraphs 3.20 to 3.22, do you have any views/comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore?"

2.4 Whilst the fact that the foreign location of an infringer of the regime may present practical limitations on the investigation and enforcement of the proposed DP law against that party is certainly a concern, we note that there is great merit in the recognition given by the European Commission that data privacy standards should apply independently of where the data is being processed. Indeed, we note, amongst other things, that:

(a) particularly where abuses concerning the handling of data over the Internet is concerned, there is precedent under Singapore law for the application of laws with “extra territorial” effect, such as section 11 of the Computer Misuse Act (Cap 50A);

(b) the advance of cloud computing and other trends in computing is part of an emerging paradigm shift where the Internet will increasingly become a place for the storage of personal information and content such that any DP regime should factor or take into account this important trend in the use, storage and processing of personal information in the digital domain;

(c) the proliferation of devices (particularly handheld, easy-to-use electronic tablets, handphones or other portable computing equipment) encourages a culture of mobility and easy access and disclosure of information which could in turn lead to potential for abuse; and

(d) the proliferation of server farms, outsourced data centres, and even the application of n-tier architecture operations have long antiquated the notion of central data processing sites.

2.5 Accordingly, notwithstanding the difficulties of enforcement, we note that there is merit in the notion providing, at the minimum, for the declaratory effect of stating that abusive practices for personal information is nevertheless illegal notwithstanding their location. Indeed, such provisions may discourage “forum shopping” and focus businesses and organisations instead on the task and need to comply with the law regardless of where their specific operations are located.

3. RULES AND EXCLUSIONS

3.1 In Question 7, MICA has asked:

> "Do you have any views/comments on the proposed general exclusions from the DP law?"

3.2 With respect to the proposed exclusion for data collected, used or disclosed by a news organisation in the course of a news activity, we are in agreement with the concept that any such exemption should be specifically limited to such news organizations as may have been declared by the Minister in charge of the DP law. In this respect, there may be merit in the view that this exclusion could be applicable only to where the collection, use, and disclosure is itself lawful. This is to ensure that the provisions continue to reasonably balance the need for compliance with the law by news organisations. Whilst we expect that major news providers, particularly in Singapore-based newspapers, will adhere to ethical and professional standards in the gathering and handling of information, there has been a proliferation of different news sources especially in the last ten years, and the growth of new media, and the result is that the landscape of participants who are potentially news organizations is a patchwork of different organizations of different profiles. As incidents in other countries have indicated, the standards, conduct and discipline over the activities of news organizations may vary. Accordingly, should the list be expanded to include foreign or non-mainstream news providers, a provision requiring lawful conduct could be an

invaluable provision to continue to ensure we provide an incentive to maintain high and ethical standards.

3.3 On the proposed exception of where personal data has been made available by a public agency to a specific organisation or the public generally, we refer to our comments at paragraph 1.3 earlier. Additionally, a comment for consideration is whether such exclusions should be limited so that the use of the information made available by the public agency is strictly excepted from the operation of the DP law only for the purposes for which the disclosure or publication was made. This is to give recognition in principle to the idea that information may be public for one purpose but should not be abused for others. In particular, this could promote or help discourage data mining practises.

3.4 In Question 10, MICA has asked:

> "Do you have any views/comments on the proposed general rules under the DP law?"

3.5 With regard to the issue of deemed or existing consent, we generally agree with the circumstances in which consent may be deemed to have been given as proposed by MICA in paragraphs 3.31 to 3.34 inclusive of the consultation paper.

3.6 However, the proposal in paragraph 3.31 contemplates that parties requesting for consent to disclosure must not seek consent for more information than is required. One comment to consider is whether this should permit scenarios where a business or organisation seeks to secure information when there is no immediate need for the specific information at the time of the request but for which, in the normal course of business, such information could be (is usually) required. An overbroad request could always be justified by information that would be “necessary” in a number of possible scenarios in the course of trade. However, to require consent to be sought for only a limited range of known purposes could result in businesses or organisations having to repeatedly contact / seek consent as and when the range of information needed evolves as part of the ordinary course of business.

3.6 A further consideration is whether the requirement to not provide misleading information in the request for consent should be balanced by a positive obligation to provide adequate disclosures of information necessary for reasonably informed consent to be obtained.

3.7 One further view to consider is whether a tougher stance is required in respect of data collection for such matters as third-party promotional activities, particularly where data is out-sourced or where it will be disclosed to third parties who are not involved in the initial collection of data.

3.8 Further, in order to not undermine the new regime, any consent given under past disclosures should not be taken into account in over-riding a customer's DNC listing.

3.9 In Question 11, MICA has asked:

> “With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or

disclose their personal data if they are notified and given reasonable time to opt out but do not?"

3.10 We note that:

(a) There may be concerns with the proposed "reasonable opt out" approach in connection with the following limited awareness / knowledge on the part of the data subject concerning the potential risks of not taking an opt out. Whilst provisions requiring non-misleading information could certainly increase the level of knowledge, there may still be a knowledge gap on the part of the data subject, or the data subject may not be able to appreciate the full risks involved in not opting out.

(b) It is not necessary to impose the proposed "deemed" consent as a matter of legislation. It may be that a balance could be struck such that the DP law requires adequate disclosure and explanation of risks (eg, via privacy policies or statements on data handling policies) but to otherwise not legislate a deeming provision which could, subject to such adequacy of disclosure of risks, be contractually provided for.

(c) If any deemed consent is proceeded with, perhaps there could be recognition of the differences between information which is "deemed" to have been consented to versus information for which there has been actual consent, ie. that deemed consent can only apply in situations where the purposes of information covered by that consent would have been reasonably inferred by a reasonable individual to whom the request was addressed (which could be in line with the position stated at paragraph 3.51 of the Consultation Paper).

3.11 In the first question numbered as Question 14 (there being a second Question 14 on page 22), MICA has asked:

"Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?|

3.12 We agree with the proposed approach as stated but note that the area of concern to businesses and organisations would most likely be in relation to what constitutes "appropriate measures" since this will likely drive compliance costs and expenses. We also note that the control over data held by third parties, particularly in outsourced scenarios (eg. cloud computing with third party service providers etc) would depend on the respective rights and obligations under the relevant agreement by which the organisation has regulated the management of the information. Taking these points collectively, the proposed obligations to ensure appropriate measures may therefore need to be tied to a concept of "reasonableness", with recognition of standards, such as those prescribed by the EU regime, but permitting inclusion or application of varying or different factors, solutions or considerations for different scenarios.

3.13 In the second question numbered as Question 14 (there being a first Question 14 on page 20), MICA has asked:

> "Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?"

3.14 With respect to paragraph 3.64 of the consultation paper, one comment for consideration relates to the standard the business or organisation in question is required to meet in discharging its obligations. Whilst we agree that "reasonable security arrangements" would be a useful benchmark, perhaps the concept of "commercially reasonable procedure" under section 17(1) and 17(2) of the Electronic Transactions Act 2010, and similar considerations detailed at section 17(2) (albeit in the context not of transactions per se but the storage, use and retention of personal information) with its emphasis on flexible factually-led enquiry as to the applicable standard, could be useful or provide guidance.

3.15 With respect to the second Question 14 as it relates to paragraph 3.66, and to Question 15 we make a comment at paragraph 3.16 below. In Question 15, MICA has asked:

> "With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?"

3.16 We note that any positive obligation to proceed with destruction of documents would need to be considered in the light of current and existing document retention requirements under law. A clear carve out under the DPA to indicate that any obligation to destroy records is to be reconciled in favour of existing mandatory document retention requirements under other law (eg, retention of relevant evidential documentation for legal proceedings) would be logical and beneficial for businesses and organisations in determining the appropriate conduct to be undertaken. Given that mandatory document retention requirements under other law are generally meant to address specific requirements, the DP law, as legislation establishing a baseline standard, could provide for a further requirement that the use of any documents retained under an exception under the DP law to meet retention periods under other legislation, be strictly limited for meeting the mandatory requirements and no other, so as to prohibit or avoid "collateral" use of such documents.

3.17 In Question 16, MICA has asked:

> "Do you have any views / comments on the proposed rules on access to and correction of personal data?"

3.18 With respect to paragraph 3.70, and the proposal that organisations may need to incur costs to allow individuals to access and correct personal data and therefore be entitled to charge a reasonable fee to recover costs, one comment for consideration is whether the right to charge should be limited only to circumstances where the individual in question has incorrectly provided the data himself/herself, as opposed to an error or mistake arising without fault of the individual, or, in the least, where the fault/error is not due to the organisation. Additionally there could be further consideration as to whether there should be a distinction between errors on entries / information provided by the data subjects themselves as opposed to third parties who have provided the information to the organisation.

4. PENALTY AND ENFORCEMENT REGIME

4.1. In Question 18, MICA has asked:

> "Do you have any views/comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views/comments on the criteria for breaches that would warrant financial penalties?"

4.2 We agree with MICA's proposal that the penalty regime should be a tiered one that will enable the DPC to enforce remedies commensurate with the seriousness of the violation. We would suggest that the criteria for determining fines should take into consideration risk, for example the number of personal records involved, whether the incident involved actual harm and if so, what sort of harm.

4.3 Additionally, we note that there may be merit in considering whether, for the purposes of proceedings or actions by the DPC, as opposed to criminal action in a court of law, there could be relevant "sentencing guidelines" which take into account an appropriate range of criminal sanctions to vary the applicable response available to the DPC. This could include a range of orders beyond fines (eg. censure, injunctive and compensation orders), with varying severity for appropriate cases (eg. stiffer sanctions for systemic abuse / infringement by an organisation or business, for flagrant breaches, and less punitive orders for minor, less culpable breaches). In this regard, it may also be useful to consider whether a past record of breaches in other incidents should be taken into account as part of the order to be made by the DPC.

5. TRANSITIONAL ARRANGEMENTS

5.1. In Question 21, MICA has asked:

> "With reference to paragraphs 4.15 to 4.19, do you have any views/comments on the proposed treatment of existing personal data?"

5.2 With respect to paragraph 4.17, we note the proposal is that consent already given by an individual for the organisation to use and/or process existing personal data could be grandfathered in (for a limited time) taking into account the nature of the organisation's business. In regard to this, we note one possible additional point that could be added is an opt out regime for the data subjects of existing personal data (ie. mandate that businesses and organisations are required to comply with any positive request for "opt out" on the use of existing personal data by the data subjects). To take the example of the after-sales customer support raised in paragraph 4.18 of the Consultation Paper, in such a context, the customer in question could request that further use of his / her information cease.

6. NATIONAL DO-NOT-CALL REGISTRY

6.1. In Question 23, MICA has asked:

"Do you have any views/comments as to whether a National Do-Not-Call registry should be set up in Singapore?"

6.2 We agree that there is great merit in the establishment of a national Do-Not-Call registry. We would suggest that it might be appropriate to finetune the registry to permit different types of permission differentiating between the different types of communications. For example, a telephone call is more intrusive than an SMS or email, so customers might not mind contact by the latter means as much as the former and may therefore wish to elect to be contacted by SMS and/or email but not by telephone.

6.3 One comment is that the national Do-Not-Call registry could itself be a valuable database depending on the fields contained in the database. We suggest that the DP law should state clearly that the data in the registry does not constitute public information and contact particulars in that data base are not therefore excluded from the definition of “personal information” by virtue solely of inclusion in the registry database.

6.4 Additionally, access to the registry database should be strictly controlled both to prevent abuse and also to provide for adequate centralized maintenance and it is proposed that this be administered by an appropriate regulatory authority where requests for confirmation / results from the database are received and resolved without providing external users rights of access to the database itself.

7. ADDITIONAL FEEDBACK

7.1 We are of the view that, generally, there are no urgent domestic concerns regarding the protection of personal data in Singapore, but that this regime is deemed necessary because of concerns within the international business community. For this reason, we are of the view that a minimalist baseline legislation as suggested by MICA is appropriate for Singapore. That said, we note that the challenges which arise in connection with regulating the use of personal information are likely to increase over time as new means of data collection, and new uses of data are developed in the course of innovation and so this legislation is also timely for this reason.

7.2 One observation here is that it may be worth considering whether the DP law proposed here should also be specially addressed or focused to protect the young (particularly minors or young children). We note that this is not without precedent in other jurisdictions (such as the Children’s Online Privacy Protection Act in the United States). Given the increasing use of electronic devices by the young in our society and various threats that could arise from the abuse of information by this segment of our society, this could be implemented within the framework of the proposed legislation, for example, in providing enhanced penalties for criminal offences in connection with a breach of the DP law where the data subject is a minor or a young child.

WongPartnership LLP
25 October 2011

ANNEX

Paragraph 1.3 – Definition of "personal information" – s6 Privacy Act 1988 of Australia

personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Paragraph 1.4 – Definition of "personal information" – s3 Privacy Act of Canada

“personal information” means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,

(ii) the title, business address and telephone number of the individual,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years.